

1과목 : 정보보호개론

- 비대칭형 암호화 방식은?
 - RC2
 - SEED
 - DES
 - Diffie-Hellman
- 안전한 Linux Server를 구축하기 위한 방법으로 옳지 않은 것은?
 - 불필요한 데몬을 제거한다.
 - 불필요한 SetUID 프로그램을 제거한다.
 - 시스템의 무결성을 주기적으로 검사한다.
 - 무결성을 검사하기 위한 데이터베이스를 추후 액세스가 용이하게 검사할 시스템에 저장하는 것이 좋다.
- IPSec 프로토콜에 대한 설명으로 옳지 않은 것은?
 - 네트워크 계층인 IP 계층에서 보안 서비스를 제공하기 위한 보안 프로토콜이다.
 - 기밀성 기능은 AH(Authentication Header)에 의하여 제공되고, 인증 서비스는 ESP(Encapsulating Security Payload)에 의하여 제공된다.
 - 보안 연계(Security Association)는 사용된 인증 및 암호 알고리즘, 사용된 암호키, 알고리즘의 동작 모드 그리고 키의 생명 주기 등을 포함한다.
 - 키 관리는 수동으로 키를 입력하는 수동방법과 IKE 프로토콜을 이용한 자동방법이 존재한다.
- 공격 유형 중 마치 다른 송신자로부터 정보가 수신된 것처럼 꾸미는 것으로, 시스템에 불법적으로 접근하여 오류의 정보를 정확한 정보인 것처럼 속이는 행위를 뜻하는 것은?
 - 차단(Interruption)
 - 위조(Fabrication)
 - 변조(Modification)
 - 가로채기(Interception)
- 암호 프로토콜 서비스에 대한 설명 중 옳지 않은 것은?
 - 비밀성 : 자료 유출의 방지
 - 접근제어 : 프로그램 상의 오류가 발생하지 않도록 방지
 - 무결성 : 메시지의 변조를 방지
 - 부인봉쇄 : 송수신 사실의 부정 방지
- WWW에서의 보안 프로토콜로 옳지 않은 것은?
 - S-HTTP(Secure Hypertext Transfer Protocol)
 - SEA(Security Extension Architecture)
 - PGP(Pretty Good Privacy)
 - SSL(Secure Sockets Layer)
- 다음 중 악성 프로그램/코드의 종류가 아닌 것은?
 - Isos
 - Stacheldraft
 - Salami
 - Convert Channel
- 대칭형 암호화 방식의 특징으로 옳지 않은 것은?
 - 처리 속도가 빠르다.
 - RSA와 같은 키 교환 방식을 사용한다.
 - 키의 교환 문제가 발생한다.
 - SSL과 같은 키 교환 방식을 사용한다.
- SET(Secure Electronic Transaction)의 기술구조에 대한 설

명으로 옳지 않은 것은?

- SET은 기본적으로 X.509 전자증명서에 기술적인 기반을 두고 있다.
 - SET에서 제공하는 인터넷에서의 안전성은 모두 암호화에 기반을 두고 있고, 이 암호화 기술은 제 3자가 해독하기가 거의 불가능하다.
 - 암호화 알고리즘에는 공개키 암호 시스템만 사용된다.
 - 이 방식은 n명이 인터넷상에서 서로 비밀통신을 할 경우 $n(n-1)/2$ 개 키를 안전하게 관리해야 하는 문제점이 있다.
- 5명의 사용자가 대칭키(Symmetric Key)를 사용하여 주고받는 메시지를 암호화하기 위해서 필요한 키의 총 개수는?
 - 2개
 - 5개
 - 7개
 - 10개

2과목 : 운영체제

- 다음 명령어 중에서 데몬들이 커널상에서 작동되고 있는지 확인하기 위해 사용하는 것은?
 - domon
 - cs
 - cp
 - ps
- 다음은 어떤 명령어에 대한 설명인가?

이 명령어는 모든 프로세스의 부모 프로세스로서 시스템 부팅 과정의 제일 마지막에 불러져서 `/etc/inittab`을 읽고 시스템의 실행레벨을 결정한다.

 - runlevel
 - init
 - nice
 - halt
- Linux에서 현재 사용하고 있는 셸(Shell)을 확인해 보기 위한 명령어는?
 - echo \$SHELL
 - vi \$SHELL
 - echo &SHELL
 - vi &SHELL
- 다음 중 `/proc`에 관한 설명으로 거리가 먼 것은?
 - 하드디스크 상에 적은 양의 물리적인 용량을 갖고 있다.
 - 만약 파일 시스템 정보를 보고자 한다면 `cat /proc/filesystems` 명령을 실행하면 된다.
 - 이 디렉터리에 존재하는 파일들은 커널에 의해서 메모리에 저장된다.
 - 이 디렉터리에는 시스템의 각종 프로세서, 프로그램정보 그리고 하드웨어 정보들이 저장된다.
- 커널의 대표적인 기능으로 옳지 않은 것은?
 - 파일 관리
 - 기억장치 관리
 - 명령어 처리
 - 프로세스 관리
- IIS 웹 서버를 설치한 다음에는 기본 웹사이트 등록정보를 수정하여야 한다. 웹사이트에 접속하는 동시 접속자수를 제한하려고 할 때 어느 부분을 수정해야 하는가?
 - 성능 탭
 - 연결 수 제한
 - 연결 시간 제한
 - 문서 탭

17. Linux 시스템 명령어 중 디스크의 용량을 확인하는 명령어는?
① cd ② df
③ cp ④ mount
18. Linux 파일 시스템의 기본 구조 중 파일에 관한 중요한 정보를 실는 곳은?
① 부트 블록 ② i-node 테이블
③ 슈퍼 블록 ④ 실린더 그룹 블록
19. vi 에디터 사용 중 명령 모드로 변환할 때 사용하는 키는?
① Esc ② Enter
③ Alt ④ Ctrl
20. 다음 명령어 중에서 시스템의 메모리 상태를 보여주는 명령어는?
① mkfs ② free
③ ps ④ shutdown
21. Linux의 기본 명령어 ‘man’의 의미는?
① 명령어에 대한 사용법을 알고 싶을 때 사용하는 명령어
② 윈도우나 셸을 빠져 나올 때 사용하는 명령어
③ 지정한 명령어가 어디에 있는지 경로를 표시
④ 기억된 명령어를 불러내는 명령어
22. DHCP(Dynamic Host Configuration Protocol) Scope 범위 혹은 주소 풀(Address Pool)을 만드는데 주의할 점에 속하지 않는 것은?
① 모든 DHCP 서버는 최소한 하나의 DHCP 범위를 가져야 한다.
② DHCP 주소 범위에서 정적으로 할당된 주소가 있다면 해당 주소를 제외해야 한다.
③ 네트워크에 여러 DHCP 서버를 운영할 경우에는 DHCP 범위가 겹치지 않아야 한다.
④ 하나의 서브넷에는 여러 개의 DHCP 범위가 사용될 수 있다.
23. Windows Server에서 FTP 서비스에 대한 설명으로 옳지 않은 것은?
① 웹 사이트가 가지고 있는 도메인을 IP Address로 바꾸어 주는 서비스를 말한다.
② IIS에서 기본적으로 제공하는 서비스이다.
③ 기본 FTP 사이트는 마우스 오른쪽 버튼을 눌러 등록정보를 수정할 수 있다.
④ FTP 서비스는 네트워크를 통하여 파일을 업로드 및 다운로드 할 수 있는 서비스를 말한다.
24. Windows Server의 DNS 서비스 설정에 관한 설명으로 옳지 않은 것은?
① 정방향 조회 영역 설정 후 반드시 역방향 조회 영역을 설정해 주어야 한다.
② Windows Server는 고정 IP Address를 가져야 한다.
③ Administrator 권한으로 설정해야 한다.
④ 책임자 이메일 주소의 at(@)은 마침표(.)로 대체된다.
25. Linux의 어떤 파일에 처음부터 끝까지 문자열 ‘her’ 를 문자열

열 'his'로 치환하되, 치환하기 전에 사용자에게 확인하여 사용자가 허락하면(y를 입력하면) 치환하고, 사용자가 허용하지 않으면 치환하지 않도록 하는 vi 명령어는?

- ① :1,\$s/her/his/gc ② :1,\$r/her/his/gc
③ :1,\$s/his/her/g ④ :1,\$r/his/her/g

26. Linux에서 네트워크 계층과 관련된 상태를 점검하기 위한 명령어와 유형이 다른 것은?
- ① ping ② traceroute
③ netstat ④ nslookup
27. Linux에서 ‘ls -al’ 명령에 의하여 출력되는 정보로 옳지 않은 것은?
- ① 파일의 접근허가 모드 ② 파일 이름
③ 소유자명, 그룹명 ④ 파일의 소유권이 변경된 시간
28. 파일의 허가 모드가 ‘-rwxr---w-’이다. 다음 설명 중 옳지 않은 것은?
- ① 소유자는 읽기 권한, 쓰기 권한, 실행 권한을 갖는다.
② 동일한 그룹에 속한 사용자는 읽기 권한만을 갖는다.
③ 다른 모든 사용자는 쓰기 권한 만을 갖는다.
④ 동일한 그룹에 속한 사용자는 실행 권한을 갖는다.
29. Linux 시스템의 shadow 파일 내용에 대한 설명으로 옳바른 것은?

```
Root:$1$SzfvKCh$dEFUonrDJZ2ZGOpqq9yK0:11458:0:99999:7:::
adm:*:11458:0:99999:7:::
lp:*:11458:0:99999:7:::
named:!:11458:0:99999:7:::
gdm:!:11458:0:99999:7:::
```

- ① lp에서 '*'은 로그인 쉘을 갖고 있으며, 시스템에 누구나 로그인할 수 있음을 의미한다.
- ② gdm에서 '!!'은 로그인 쉘을 갖고 있지만 누구도 계정을 통해서 로그인할 수 없도록 계정이 잠금 상태라는 것을 의미한다.
- ③ 로그인 계정이 아닌 시스템 계정은 named와 gdm 이다.
- ④ root의 암호는 11458 이다.

30. Windows Server에서 감사정책을 설정하고 기록을 남길 수 있는 그룹은?
- ① Administrators ② Security Operators
③ Backup Operators ④ Audit Operators

3과목 : 네트워크

31. TCP와 UDP의 차이점을 설명한 것 중 옳지 않은 것은?
- ① TCP는 전달된 패킷에 대한 수신측의 인증이 필요하지만 UDP는 필요하지 않다.
 - ② TCP는 대용량의 데이터나 중요한 데이터 전송에 이용되지만 UDP는 단순한 메시지 전달에 주로 사용된다.
 - ③ UDP는 네트워크가 혼잡하거나 라우팅이 복잡할 경우에는 패킷이 유실될 우려가 있다.
 - ④ UDP는 데이터 전송 전에 반드시 송수신 간의 세션이 먼저 수립되어야 한다.
32. 네트워크 주소 중 B Class 기반의 IP Address로 옳지 않은 것은?

- ① 139.39.60.101 ② 203.34.1.12
③ 187.124.70.87 ④ 155.98.200.100
33. 전송을 받는 개체 발송지에서 오는 데이터의 양이나 속도를 제한하는 프로토콜의 기능은?
① 에러제어 ② 순서제어
③ 흐름제어 ④ 접속제어
34. IPv4에 비하여 IPv6이 개선된 것에 대한 설명으로 잘못된 것은?
① 128bit 구조를 가지기 때문에 기존의 IPv4 보다 더 많은 노드를 가질 수 있다.
② 전역방송(Broad Cast)이 가능하다.
③ IPv6에서는 확장이 자유로운 가변길이 변수로 이루어진 옵션 필드 부분 때문에 융통성이 발휘된다.
④ IPv6에서는 Loose Routing과 Strict Routing의 두 가지 옵션을 가지고 있다.
35. 다음과 같은 일을 수행하는 프로토콜은?
- 인터넷에 접속한 호스트들은 인터넷 주소에 의해서 식별되지만 실질적인 통신은 물리적인 네트워크 주소를 얻어야 가능하다.
- ① DHCP(Dynamic Host Configuration Protocol)
② IP(Internet Protocol)
③ RIP(Routing Information Protocol)
④ ARP(Address Resolution Protocol)
36. OSI 7 Layer에서 암호/복호, 인증, 압축 등의 기능이 수행되는 계층은?
① Transport Layer ② Datalink Layer
③ Presentation Layer ④ Application Layer
37. TCP 헤더 필드의 내용으로 옳지 않은 것은?
① TTL(Time To Live) ② 발신지 포트번호
③ 윈도우 크기 ④ Checksum
38. 네트워크 관리자나 라우터가 IP 프로토콜의 동작 여부를 점검하고, 호스트로의 도달 가능성을 검사하기 위한 ICMP 메시지 종류는?
① Parameter Problem
② Timestamp Request/Response
③ Echo Request/Response
④ Destination Unreachable
39. 다음 프로토콜 중 OSI 7 Layer 계층이 다른 프로토콜은?
① ICMP(Internet Control Message Protocol)
② IP(Internet Protocol)
③ ARP(Address Resolution Protocol)
④ TCP(Transmission Control Protocol)
40. 아래 내용에 해당하는 서브넷 마스크 값은?
- 203.76.25.1/26
- ① 255.255.255.192 ② 255.255.255.224

- ③ 255.255.255.254 ④ 255.255.255.0
41. 데이터 링크 오류제어를 위한 ARQ 방식 중 오류가 발생한 프레임만을 재전송하는 방식으로 전송 성능이 가장 우수한 것은?
① Stop-and-Wait ARQ
② Go-back-N ARQ
③ Selective Repeat ARQ
④ 모든 ARQ는 전송 성능이 동일하다.
42. 홉 카운팅 기능을 제공하는 라우팅 프로토콜은?
① SNMP ② RIP
③ SMB ④ OSPF
43. TCP/IP 프로토콜을 이용해서 서버와 클라이언트가 통신을 할 때, 'netstat' 명령을 이용해 현재의 접속 상태를 확인할 수 있다. 클라이언트와 서버가 현재 올바르게 연결되어 통신 중인 경우 'netstat'으로 상태를 확인하였을 때 나타나는 메시지는?
① SYN_PCVD ② ESTABLISHED
③ CLOSE_WAIT ④ CONNECTED
44. TCP는 연결 설정과정에서 3-way handshaking 기법을 이용하여 호스트 대 호스트의 연결을 초기화한다. 다음 중 호스트 대 호스트 연결을 초기화할 때 사용되는 패킷은?
① SYN ② RST
③ FIN ④ URG
45. 서브넷 마스크에 대한 설명으로 옳바른 것은?
① DNS 데이터베이스를 관리하고 IP Address를 DNS의 이름과 연결한다.
② IP Address에 대한 네트워크를 분류 또는 구분한다.
③ TCP/IP의 자동설정에서 사용되는 프로토콜로서 정적, 동적 IP Address를 지정하고 관리한다.
④ 서로 다른 네트워크를 연결할 때 네트워크 사이를 연결하는 장치이다.
- 4과목 : 보안**
46. HTTP Session Hijacking 공격 방법으로 옳지 않은 것은?
① 공격자는 Session을 가로채기 위해 웹 서버와 웹 클라이언트의 트래픽을 직접적으로 Sniffing하는 방법
② 웹 서버 상에 공격 코드를 삽입하고 사용자의 실행을 기다리는 방법
③ Session ID 값을 무작위 추측 대입(Brute-Force Guessing)함으로써 공격하는 방법
④ 웹 서버의 서비스를 중단 시키고, 공격자가 서버에 도착하는 모든 패킷을 가로채는 방법
47. 웹 해킹의 한 종류인 SQL Injection 공격은 조작된 SQL 질의를 통하여 공격자가 원하는 SQL구문을 실행하는 기법이다. 이를 예방하기 위한 방법으로 옳지 않은 것은?
① 에러 감시와 분석을 위해 SQL 에러 메시지를 웹상에 상세히 출력한다.
② 입력 값에 대한 검증을 실시한다.
③ SQL 구문에 영향을 미칠 수 있는 입력 값은 적절하게 변환한다.

- ④ SQL 및 스크립트 언어 인터프리터를 최신 버전으로 유지한다.
48. 버퍼 오버플로우(Buffer Overflow)의 설명으로 옳지 않은 것은?
- ① 지정된 버퍼의 크기보다 더 많은 데이터를 입력해서 프로그램이 비정상적으로 동작하도록 만드는 것을 의미함
 - ② 대부분의 경우 버퍼가 오버플로우 되면 프로그램이 비정상적으로 종료되면서 루트 권한을 획득할 수 있음
 - ③ 버퍼가 오버플로우 되는 순간에 사용자가 원하는 임의의 명령어를 수행시킬 수 있음
 - ④ 버퍼 오버플로우를 방지하기 위해서는 시스템에 최신 패치를 유지해야 함
49. SSL(Secure Socket Layer)의 설명 중 옳지 않은 것은?
- ① SSL에서는 키 교환 방법으로 Diffie_Hellman 키 교환방법만을 이용한다.
 - ② SSL에는 Handshake 프로토콜에 의하여 생성되는 세션과 등위간의 연결을 나타내는 연결이 존재한다.
 - ③ SSL에서 Handshake 프로토콜은 서버와 클라이언트가 서로 인증하고 암호화 MAC 키를 교환하기 위한 프로토콜이다.
 - ④ SSL 레코드 계층은 분할, 압축, MAC 추가, 암호 등의 기능을 갖는다.
50. 다음에서 설명하는 기법은?

인터넷 프로토콜인 TCP/IP의 구조적 결함, 즉 TCP 시퀀스번호, 소스라우팅, 소스 주소를 이용한 인증(Authentication) 기능을 가지고 있는 시스템에 침입하기 위해 침입자가 사용하는 시스템을 원래의 호스트로 위장하는 방법이다.

- ① IP Sniffing ② IP Spoofing
 - ③ Race Condition ④ Packet Filtering
51. SYN 플러딩 공격에 대한 설명으로 옳바른 것은?
- ① TCP 프로토콜의 3-way handshaking 방식의 접속 문제점을 이용하는 것으로, IP 스푸핑 공격을 위한 사전 준비 단계에서 이용되는 공격이며, 서버가 클라이언트로부터 과도한 접속 요구를 받아 이를 처리하기 위한 구조인 백로그(backlog)가 한계에 이르러 다른 클라이언트로부터 오는 새로운 연결 요청을 받을 수 없게 하는 공격이다.
 - ② 함수의 지역 변수에 매개변수를 복사할 때 길이를 확인하지 않은 특성을 이용하는 공격 방법이다.
 - ③ 네트워크에 연결된 호스트들의 이용 가능한 서비스와 포트를 조사하여 보안 취약점을 조사하기 위한 공격방법이다.
 - ④ 패킷을 전송할 때 암호화하여 전송하는 보안 도구이다.
52. 다음은 어떤 보안 도구를 의미하는가?
- 회사의 사설 네트워크와 외부의 공중 네트워크 사이의 중립 지역으로써 삽입된 컴퓨터 호스트 또는 소형 네트워크를 말한다.
- ① IDS ② DMZ
 - ③ Firewall ④ VPN

53. 다음 명령에 대한 설명으로 옳바른 것은?
- ① #chmod g-w : 그룹에게 쓰기 권한 부여
 - ② #chmod g-rwx : 그룹에게 읽기, 쓰기, 실행 권한 부여
 - ③ #chmpd a+r : 그룹에게만 읽기 권한 부여
 - ④ #chmod g+rw : 그룹에게 대해 읽기, 쓰기 권한 부여
54. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?
- ① 안전하지 못한 네트워크에서 안전하게 통신할 수 있는 기능과 강력한 인증방법을 제공한다.
 - ② 문자를 암호화하여 IP Spoofing, DNS Spoofing으로부터 보호할 수 있다.
 - ③ 쌍방 간 인증을 위해 Skipjack 알고리즘이 이용된다.
 - ④ 네트워크의 외부 컴퓨터에 로그인 할 수 있고 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 프로그램이다.
55. PGP(Pretty Good Privacy)에서 지원하지 못하는 기능은?
- ① 메시지 인증 ② 수신 부인방지
 - ③ 사용자 인증 ④ 송신 부인방지
56. Windows Server의 이벤트뷰어에서 중요 로그 유형에 해당하지 않은 것은?
- ① Firewall Log ② Security Log
 - ③ System Log ④ Application Log
57. Linux에서 각 사용자의 가장 최근 로그인 시간을 기록하는 로그 파일은?
- ① cron ② messages
 - ③ netconf ④ lastlog
58. 대형 응용 프로그램을 개발하면서 전체 시험실행을 할 때 발견되는 오류를 쉽게 해결하거나 처음부터 중간에 내용을 볼 수 있는 부정루틴을 삽입해 컴퓨터의 정비나 유지 보수를 핑계 삼아 컴퓨터 내부의 자료를 뺏아가는 해킹 행위는?
- ① Trap Door ② Asynchronous Attacks
 - ③ Super Zapping ④ Salami Techniques
59. Windows 명령 프롬프트 창에서 'netstat -an' 을 실행한 결과이다. 옳지 않은 것은?(단, 로컬 IP Address는 211.116.233.104 이다.)

```
c:\W>netstat -an

TCP 127.0.0.1:80 127.0.0.1:1197 TIME_WAIT
TCP 127.0.0.1:80 127.0.0.1:1200 ESTABLISHED
TCP 127.0.0.1:1200 127.0.0.1:80 ESTABLISHED
TCP 211.116.233.104:139 0.0.0.0:0 LISTENING
TCP 211.116.233.104:22 211.116.233.98:22 ESTABLISHED
TCP 211.116.233.104:23 211.116.233.124:2212 TIME_WAIT
```

- ① http://localhost 로 접속하였다.
- ② NetBIOS를 사용하고 있는 컴퓨터이다.
- ③ 211.116.233.124에서 Telnet 연결이 이루어져 있다.
- ④ 211.116.233.98로 ssh를 이용하여 연결이 이루어져 있다.

60. 스머프 공격(Smurf Attack)에 대한 설명으로 옳바른 것은?
- ① 두 개의 IP 프래그먼트를 하나의 데이터그램인 것처럼 하여 공격 대상의 컴퓨터에 보내면, 대상 컴퓨터가 받은 두 개의 프래그먼트를 하나의 데이터그램으로 합치는 과정에서 혼란에 빠지게 만드는 공격이다.
 - ② 서버의 버그가 있는 특정 서비스의 접근 포트로 대량의 문자를 입력하여 전송하면, 서버의 수신 버퍼가 넘쳐서 서버가 혼란에 빠지게 만드는 공격이다.
 - ③ 서버의 SMTP 서비스 포트로 대량의 메일을 한꺼번에 보내고, 서버가 그것을 처리하지 못하게 만들어 시스템을 혼란에 빠지게 하는 공격이다.
 - ④ 출발지 주소를 공격하고자 하는 컴퓨터의 IP Address로 지정한 후 패킷신호를 네트워크 상의 컴퓨터에 보내게 되면 패킷을 받은 컴퓨터들이 반송 패킷을 다시 보내게 되는데, 이러한 원리를 이용하여 대상 컴퓨터에 갑자기 많은 양의 패킷을 처리하게 함으로써 시스템을 혼란에 빠지게 하는 공격이다.

전자문제집 CBT PC 버전 : www.comcbt.com
전자문제집 CBT 모바일 버전 : m.comcbt.com
기출문제 및 해설집 다운로드 : www.comcbt.com/x

전자문제집 CBT란?
종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.
PC 버전 및 모바일 버전 완벽 연동
교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

1	2	3	4	5	6	7	8	9	10
④	④	②	②	②	③	①	②	③	④
11	12	13	14	15	16	17	18	19	20
④	②	①	①	③	②	②	②	①	②
21	22	23	24	25	26	27	28	29	30
①	④	①	①	①	④	④	④	②	①
31	32	33	34	35	36	37	38	39	40
④	②	③	②	④	③	①	③	④	①
41	42	43	44	45	46	47	48	49	50
③	②	②	①	②	④	①	②	①	②
51	52	53	54	55	56	57	58	59	60
①	②	④	③	②	①	④	①	③	④